



NCRA 2018:  
The Changing  
Art and  
Architecture of  
Utility  
Regulation

# Issues to Consider When Collecting Cybersecurity Information from Utilities

Dominic Saebeler

Wei Chen Lin



## Disclaimer

The views and opinions expressed herein strictly represent those of the presenters at this moment, and may not necessarily agree with positions of ICC Commissioners or Commission Staff. The presenters reserve the right to change those views and opinions as new information becomes available.



4.25.18  
Discussion  
Topics

- I. Introduction to Information Security
- II. Complexities of Contemporary Utility Operations
- III. What is Critical Infrastructure Information (CII)?
- IV. Interaction between a PUC and a Utility
- V. Existing Legal Protections for CII
- VI. Possible Solutions
- VII. Questions

# Introduction to Information Security

## CIA Triad

Information kept must be available only to authorized individuals

Confidentiality

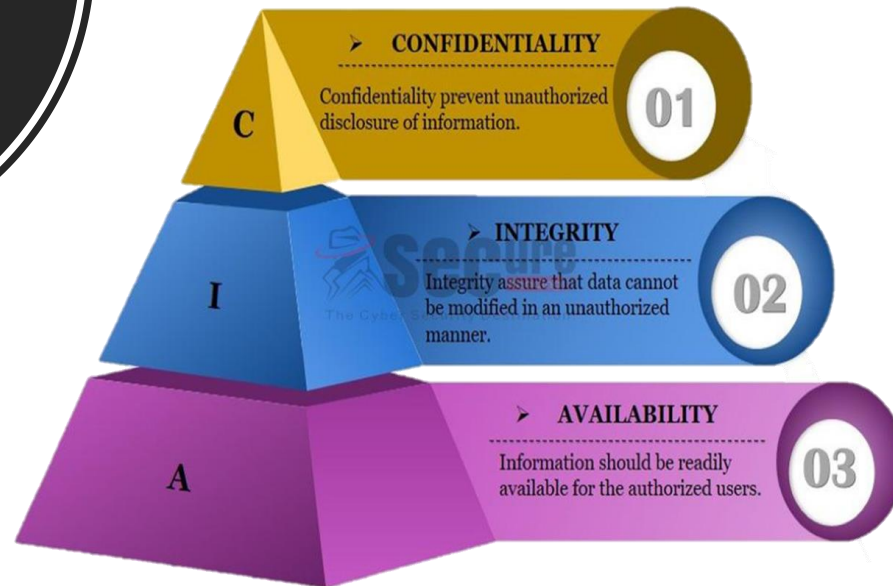
Unauthorized changes must be prevented

Integrity

Information Security

Availability

Authorized users must have access to their information for legitimate purposes



## The CIA Triad

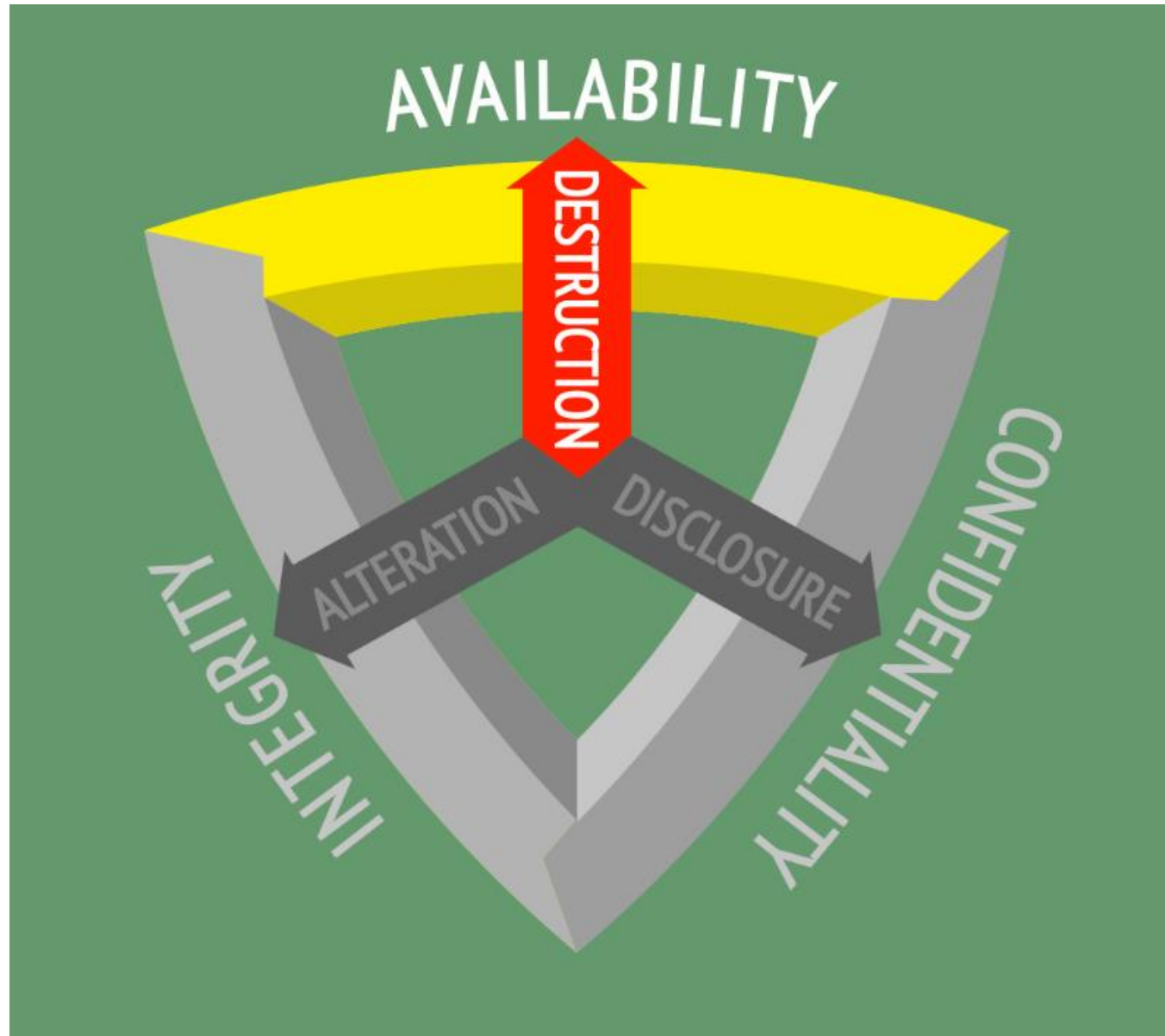
**Confidentiality**  
The state of being secret

**Security**

**Integrity**  
The state or quality of being entire or complete

**Availability**  
Present and ready for use

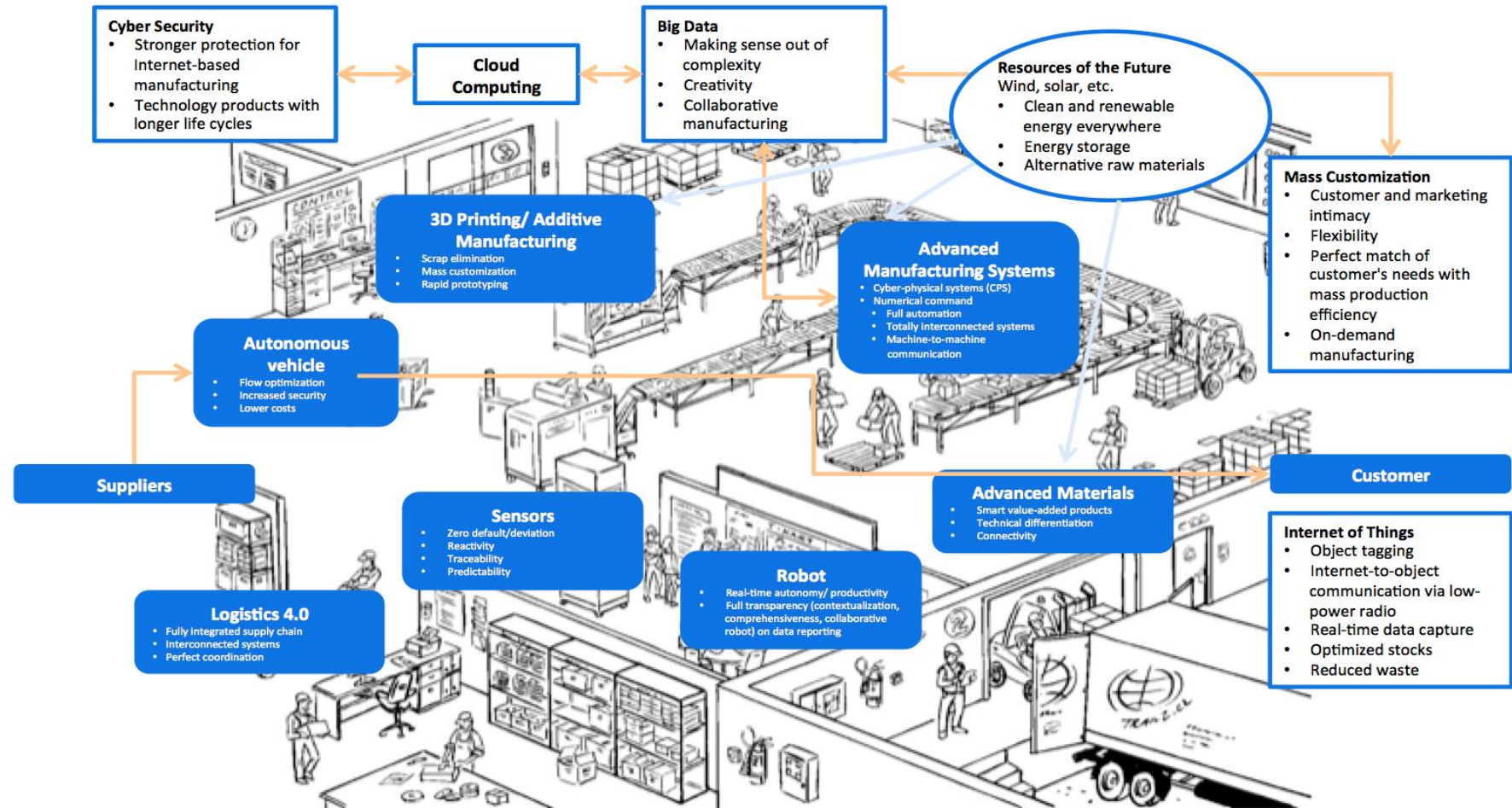
How  
Confidentiality,  
Integrity, and  
Availability can  
be  
Compromised



The  
Challenge of  
Handling  
SCADA  
Information



# Increasingly Complex Information Rich Environment



Governments  
Add Risk to  
Data  
Protection

## NUMBER OF RECORDS BREACHED BY INDUSTRY IN FIRST HALF OF 2017



**1,901,866,611 TOTAL RECORDS**

Source: BREACHLEVELINDEX.COM  
January 2017 to June 2017

Governments  
Add Risk to  
Data  
Protection



## U.S. Government Contractors Score Poorly on Cyber Risk Tests

### Report Analyzes Cyber Risk of Federal Supply Chain

Attacks against the supply chain are not uncommon. It represents the soft underbelly of large organizations that are otherwise well defended. The federal government is not an exception -- in fact, federal agencies are especially reliant on their supply chain; and the security posture of that supply chain is of national importance.

### Ways to access PUC held information:

- Unintentional Disclosure
  - Breach
  - Insecure Transfer
- Intentional Disclosure
  - FOIA
  - Litigation

Governments  
Add Risk to  
Data  
Protection



**BRIEF**

## **FERC among targets of Iranian hackers charged by DOJ**

## Who are the Adversaries?

### Ransomware Is Big Business

Ransomware netted cyber-criminals more than \$1 billion last year, mostly from individuals and small businesses. The technique of locking or encrypting files and then demanding ransom for the key is an evolution of traditional cyber-crime business models of merely stealing data or taking down networks. Those methods take a lot of effort and don't always deliver a lot of money, if any.

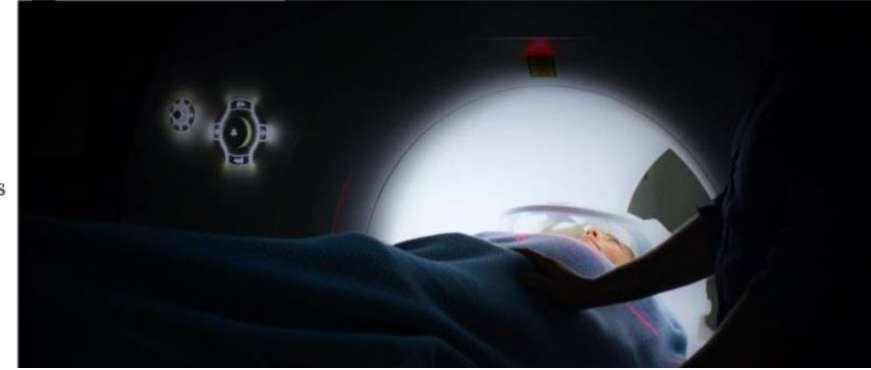
### Critical Infrastructure on the Hit List

Over the past few years at the Black Hat conference, researchers have shown ways hackers have compromised everything from cars to door locks to guns and every internet of things (IoT) device in between. Ransomware changes the dynamics of these hacks significantly, to the point where the nation's critical infrastructure will be held for ransom.

### Attack Scenarios

According to the National Security Telecommunications Advisory Committee Information Assurance Task Force, open sources (including the Internet, FERC filings, electric industry publications, and regional maps) would provide sufficient information to enable hackers to identify the most heavily used transmission lines and most critical substations in the power grid. Relatively simple techniques could be used to locate the appropriate dial-in ports to these points and modify settings to trigger an outage. At that point, only a detailed review of the log or eliminating all other factors would result in the detection of this type of attack.<sup>4</sup> This means that a “script-kiddie” that has done his homework could indeed conceivably take down at least a section of the power grid.

### Cyberterrorists targeting healthcare systems, critical infrastructure



Who are the  
Adversaries?

## Experts: North Korea Targeted U.S. Electric Power Companies

by ANDREA MITCHELL and KEN DILANIAN

WASHINGTON — The cybersecurity company FireEye says in a new report to private clients, obtained exclusively by NBC News, that hackers linked to North Korea recently targeted U.S. electric power companies with spearphishing emails.

The emails used fake invitations to a fundraiser to target victims, FireEye said. A victim who downloaded the invitation attached to the email would also be downloading malware into his or her computer network, according to the FireEye report. The company did not dispute NBC's characterization of the report, but declined to comment.

There is no evidence that the hacking attempts were successful, but FireEye assessed that the targeting of electric utilities could be related to increasing tensions between the U.S. and North Korea, potentially foreshadowing a disruptive cyberattack.



## Chinese Army Hackers Are Trying to Bring Down U.S. Infrastructure, After All

Remember [that scary column Obama wrote last year](#), describing the nightmarish scenario of a crippling cyber attack that shut down our power grid and poisoned our water? It just got real.



## Russia-backed hackers try to hijack Britain's power supply



What the  
Adversaries  
Want to Know /  
What They  
Might Already  
Know?

## How utilities are securing their systems

- Mitigation strategies
- COOP and other response plans, playbooks
- Training materials
- Schematics and Blueprints



## What specific devices are used by the utilities

- Whether they contain any vulnerabilities
- Example: DragonFly 2.0 Campaign – Searched Publicity Photos (revealed type and status of equipment)

## Where the gaps are

- Results of: Risk assessments, vulnerability assessments, and sources of threat data
- Interdependencies

## Attacker Methodology

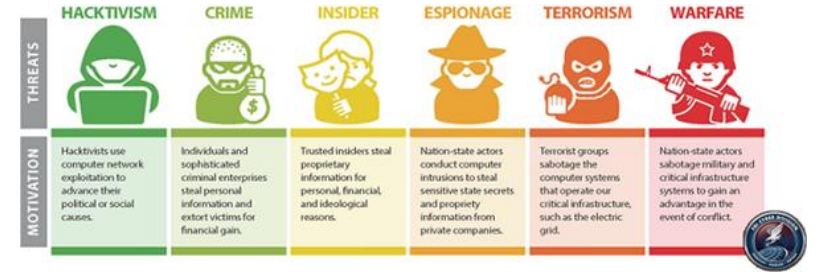
# Attacker's Methodology



## Attacker Methodology,

### Performing Reconnaissance

- Network
- Technology
- Business Process
  - How personnel operate
    - Emails and calendar entries
- Security priorities
  - “If an adversary knows, for example, that a company’s security team is measured by how quickly it remediates incidents, an attack may include malware that’s easy to discover as a way to distract them from the real operation.”



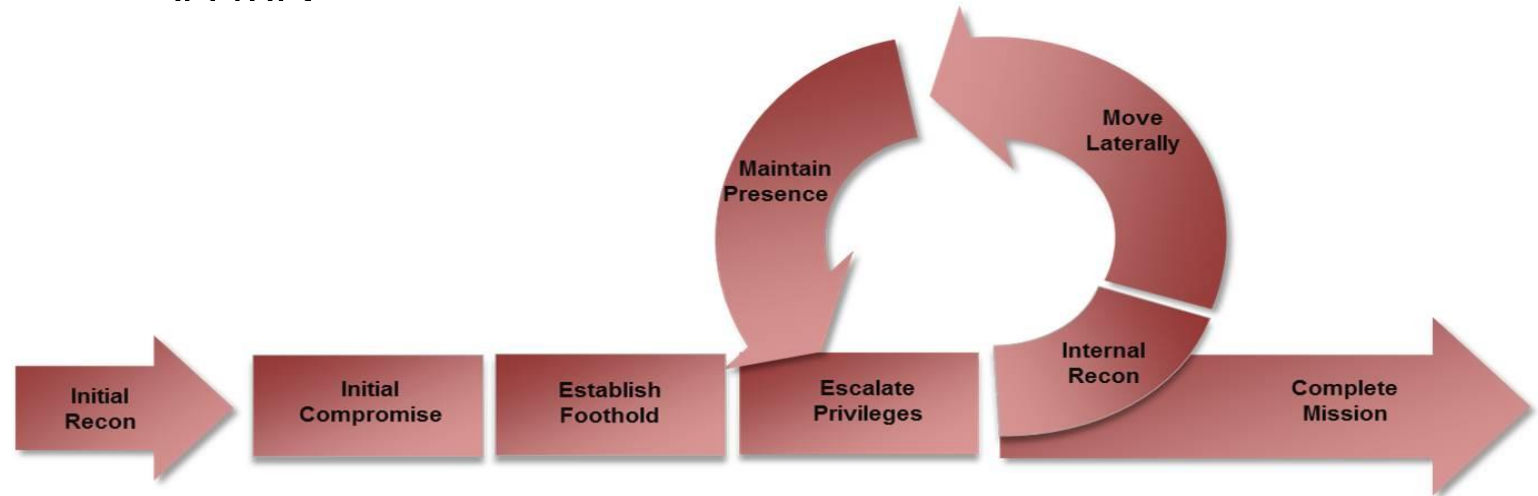
### Scanning and enumeration

- Passive information gathering
- Active information gathering
- Open-source reconnaissance: gathering information posted on company-controlled websites.

## Attacker Methodology, Recon Cont.

### Scanning and enumeration Cont.

- Open-source reconnaissance: gathering information posted on company-controlled websites.
  - “In some cases, information posted to company websites, especially information that may appear to be innocuous, may contain operationally sensitive information. As an example, the threat actors downloaded a small photo from a publicly accessible human resources page. The image, when expanded, was a high-resolution photo that displayed control systems equipment models and status information in the background.” **TA18-074A: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors**



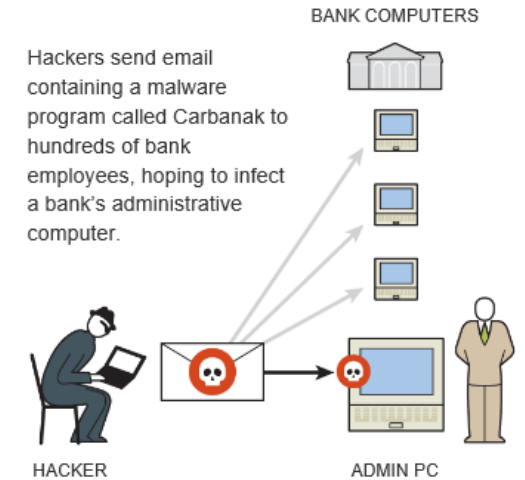
Even Seemingly  
Mundane  
Business  
Process  
Information  
can be  
Sensitive

## Reported hacks on Russian banks

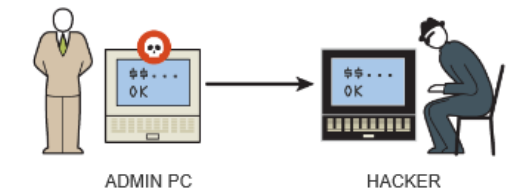
- After gaining access to the systems, the attackers monitored the compromised computers to learn bank procedures over months.
- “The goal was to mimic their activities . . . that way, everything would look like a normal, everyday transaction”

### How Hackers Infiltrated Banks

Since late 2013, an unknown group of hackers has reportedly stolen \$300 million — possibly as much as triple that amount — from banks across the world, with the majority of the victims in Russia. The attacks continue, all using roughly the same modus operandi:



Programs installed by the malware record keystrokes and take screen shots of the bank's computers, so that hackers can learn bank procedures. They also enable hackers to control the banks' computers remotely.



By mimicking the bank procedures they have learned, hackers direct the banks' computers to steal money in a variety of ways:

Why would a  
PUC want to  
Collect  
Cybersecurity  
Information  
from Utilities?

## **Dated but Valuable Reference:** 2007 NARUC – Information Sharing Practices in Regulated Critical Infrastructure State Analysis and Recommendations

### Generally

- Rate cases
- Siting applications
- Required periodic reporting
- Incident reporting

### Specific to Cybersecurity:

- Responsible for knowing what is going on
- Ensuring they are doing enough
- Driving them to do more
- Peer assessment, helping them compare to each other



What  
Information  
does the PUC  
want to  
Collect?

## How utilities are securing their systems

- Mitigation strategies
- COOP and other response plans, playbooks
- Training materials
- Schematics and Blueprints

## What specific devices are used by the utilities

- Whether they contain any vulnerabilities

## Where the gaps are

- Results of: Risk assessment, vulnerability assessment, sources of threat data
- Interdependencies

## Does this Look Familiar?



Why this  
Matters?

## The need for information

- “The key to keeping the system running is not only adequate investment and physical protection of the systems from disasters, but also trusted communication about vulnerabilities, threats, and recovery procedures”

## The need for cooperation

- “Utility commissions can only do their job well if the companies they regulate share information with them in an atmosphere of trust and confidence, and the regulated companies may be reluctant to initiate a rate case if they feel that it will likely require them to divulge sensitive information about their systems.”



## Information Sources

# ESCC

Electricity Subsector  
Coordinating Council



Homeland  
Security

Protected Critical Infrastructure  
Information Program



# IEMA



# US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM



ONG-ISAC



What  
Information  
does the PUC  
want to  
Collect?

## How Specific?

- Standards, Frameworks, Programs
- Strategies
- Procedures
- Network topography
- . . . down to . . .
- Devices
  - Vendors
  - Models
- Software versions
- Configurations

**Recall earlier slide:** “If an adversary knows, for example, that a company’s security team is measured by how quickly it remediates incidents, an attack may include malware that’s easy to discover as a way to distract them from the real operation.”

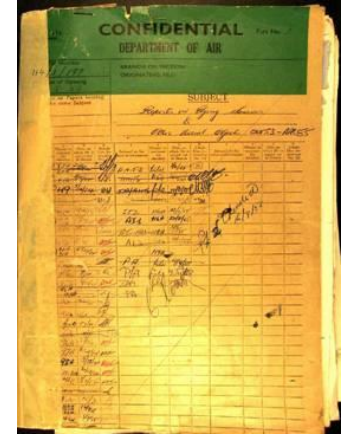
# How to Protect from Unintentional Disclosure? Technical

## What to collect?

- How granular?
  - What not to collect?

## How to collect?

- Written?
- Briefings?
  - Honor system, Chatham house rule?
  - NDA?



## How to Store?

- Digital
  - IT Security?
- Paper
  - Physical Security?
- (how long?)



## Who has access?

- Insider threat

## How often to review process for collection

- Training
- Petrify/cement institutional knowledge

How to Protect  
Against  
Intentional  
Disclosure?  
Legal

## Common law

- Displaced by Federal FOIA
- Alive in limited circumstances in the states?

## Statutory

- Freedom of Information, Open Records, Sunshine, Right to Know, etc.

## Rules of Evidence

- In litigation

## Administrative rules

- In administrative proceedings
  - How does ALJ decide?
    - Protective orders?
  - What is in the administrative procedures in each state?



# FOIA

## Analysis

- Public record?
- Exemption?
  - Specific Exemptions
    - Definition of critical infrastructure information?
  - Exemptions with reference to federal law?
  - Exemptions in the interest of general health and security of the public?
  - Extension of commercial and proprietary information?
  - Catch-all?



## Landscape

- Federal FOIA, PCII Program (6 CFR 29.8)
  - “PCII is made available only to those federal, state, tribal, and local government employees and their contractors who:
    - “Are trained in the proper handling and safeguarding of PCII.”
    - “Have homeland security responsibility as specified in the Critical Infrastructure Information (CII) Act of 2002, the Final Rule, and the policies and procedures issued by the PCII Program.”
    - “Have a need to know the specific information.”
    - “Sign a Non-Disclosure Agreement (nonfederal employees).”
- State
  - “State FOIA Laws are not generally superseded or limited by Federal law.”

Case Law  
from Various  
Jurisdictions

Northwest Gas Ass'n v. Washington Utilities  
and Transp. Com'n, 141 Wash.App. 98 (2007)


County of Santa Clara v. Superior Court, 170  
Cal.App.4th 1301 (2009)

Office of People's Counsel v. Public Service  
Com'n, 21 A.3d 985 (2011)

Crawford v. New York City Dept. of Information  
Technology, 43 Misc.3d 735 (2014)

Smith on behalf of Smith Butz, LLC v.  
Pennsylvania, 161 A.3d 1049 (2017)





Moving  
Forward

- Federal PCII Program (<https://www.dhs.gov/pcii-program>)
- State FOIA Legislation
- Administrative Rules / Procedures
- Create entity within state responsible for received CII (e.g. NJCCIC) (“Bailee”?)

## Sources / Image Credits

- <http://pubs.naruc.org/pub/536E206C-2354-D714-515A-81819AA70A02>
- <https://securereading.com/infobasics-basic-concept-information-security/>
- Michael G. Solomon, Information Security Illuminated 3 (2005)
- <http://www.abc.net.au/news/2017-10-23/forget-explosives,-terrorists-are-coming-after-cyber-systems/9076786>
- <http://www.eweek.com/security/ransomware-becoming-bigger-threat-for-businesses-critical-infrastructure>
- <http://www.awwaneb.org/pdfs/securityprivacy.pdf>
- <http://www.pearsonitcertification.com/articles/article.aspx?p=462199&seqNum=2>
- <https://www.csoononline.com/article/3075827/security/components-of-modern-hacking-operations.html>
- <https://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html>
- <https://www.sans.org/reading-room/whitepapers/hackers/hackers-turn-lights-off-vulnerability-power-grid-electronic-attack-606>
- <https://www.us-cert.gov/ncas/alerts/TA18-074A>
- <https://www.eenews.net/stories/1060077389>
- <https://www.utilitydive.com/news/ferc-among-targets-of-iranian-hackers-charged-by-doj/519875/>
- <https://www.jasondion.com/>
- <https://www.7sec.com/know/ddos-stress-testing/>



**SOURCES  
LISTED!**